Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
	)	
Call Authentication Trust Anchor	)	WC Docket No. 17-97

COMMENTS OF TWILIO INC.

Twilio, Inc.[1] is pleased to comment on the Commission's Third Further Notice of Proposed Rulemaking on matters related to the implementation of the SHAKEN/STIR Caller ID identification framework.[2]

I. INTRODUCTION AND SUMMARY

Twilio strongly supports the Commission's goal of curbing unlawful robocalls. Unlawful robocalls erode faith in the public telephone network and harm consumers, and Caller ID authentication is an important part of the solution to unlawful robocalls. Twilio accordingly has devoted substantial resources to keeping bad actors—including parties engaged in fraudulent spoofing—off of its platform. Against that backdrop, Twilio offers three core recommendations to the Commission concerning the implementation of SHAKEN/STIR.

---

[1] Twilio Inc. offers cloud communications services that allow software developers to embed voice, text, chat, email, and video into web and mobile applications. Since its founding in 2008, Twilio has grown to a company of more than 2000 employees, with offices in Europe, Asia, and Latin America, in addition to the United States. Today, Twilio powers more than 600 billion annualized interactions every year and helps more than 150,000 customers, from small businesses to the world's largest multinational companies, from industries including education, healthcare, manufacturing, public safety, financial services, and many more reinvent how they engage with their customers or constituents.

[2] *Advanced Methods to Target and Eliminate Unlawful Robocalls; Call Authentication Trust Anchor*, Declaratory Ruling and Third Further Notice of Proposed Rulemaking, FCC 19-51, CG Docket No. 17-59, WC Docket No. 17-97 (rel. June 7, 2019) ("Declaratory Ruling" or "FNPRM").

First, Twilio agrees that the Commission should facilitate the deployment of SHAKEN/STIR by adopting the proposed safe harbor for blocking of calls with complete attestation information that fail authentication under SHAKEN/STIR. The scope of the proposed safe harbor recognizes that it may be reasonable to block a call when it has complete attestation information but fails authentication; in such cases, the attestation header likely will have been maliciously altered or created. The Commission is right, however, not to extend the safe harbor to calls lacking complete attestation information. Attestation information may be incomplete for any number of innocent reasons, including for calls that pass through a TDM-based network or originate from carriers that interconnect with other carriers in TDM—as is the case for many calls in rural areas. Blocking calls in these cases would uniquely disadvantage rural carriers and the consumers and businesses they serve. As one of the principal technologists for ATIS, Jim McEachern, succinctly put it in encouraging a methodical approach to implementation of SHAKEN/STIR: "You want to proceed in a very measured way to make sure that you don't hurt things by trying to help things."[3]

Second, to ensure that the safe harbor achieves the goal of encouraging responsible deployment of SHAKEN/STIR, Twilio supports limiting the safe harbor to circumstances where the voice service provider has provided a mechanism for identifying and remedying the blocking of wanted calls. This will ensure that consumers are in the driver's seat, empowering them to choose which calls they do or do not want to receive and preventing the blocking of legitimate calls. Voice service providers similarly should provide a means for callers to know when their calls have been blocked, including through the sending of a unique SIP code, together with a

[3] Carol Wilson, *Robocall Fix Not a Silver Bullet*, LightReading (Dec. 13, 2018), https://www.lightreading.com/services/voip-services/robocall-fix-not-a-silver-bullet/d/d-id/748282.

mechanism for obtaining prompt remediation of erroneously blocked or mis-labeled calls.

Third, Twilio supports establishing a "Critical Calls List" to prevent the blocking of emergency calls. This protection should extend not just to calls to or from 911 call centers, but also to calls intended to provide important information to the public that relates to the safety of life or property. So that industry and other stakeholders can develop the right approach to the Critical Calls List, Twilio encourages the Commission to refer development of a Critical Calls List to the North American Numbering Council.

II. TWILIO STANDS WITH THE COMMISSION IN THE FIGHT AGAINST UNLAWFUL ROBOCALLS.

Twilio's services allow software developers to embed voice communications capabilities in their applications, enabling companies and organizations to communicate more efficiently and effectively with their customers. More than five million developers have built applications using Twilio, embedding communications in applications that allow users to contact their teacher or students, alert their constituents about an emergency, hail a ride, make a bank transaction, shop online, authenticate an account, or contact elected officials.

As a facilitator of trusted communications, Twilio takes seriously the threat that unlawful robocalls pose to its customers and to the public at large, and it is an active participant in the fight against the bad actors who place such calls. For example, Twilio has adopted a number of safeguards that prevent unlawful robocalls into or coming from its platform.[4] Among other safeguards, Twilio:

- Requires customers to demonstrate that they own a phone number before allowing the number to be used as a caller ID when initiating a phone call via its APIs.

[4] Jeff Lawson, *Your Phone, Your Call - Part I - Eliminating Robocalls*, Twilio Blog (Mar. 18, 2019), https://www.twilio.com/blog/your-phone-your-call-eliminating-robocalls.

- Bills by the minute, rather than by the second, in order to deter short-duration calls and impair the economics of unlawful robocalls.
- Disables calls to high-fraud destinations that are rarely used for legitimate use-cases, using a system of geographic permissions.
- Imposes default throughput limits, which means that an entity that recently became a customer cannot immediately place a high volume of calls or send a high volume of messages.
- Uses artificial intelligence and data analytics to identify risk vectors, monitor patterns that might indicate abuse, and respond to complaints.
- Is piloting know-your-customer policies, in partnership with two companies that carriers use for spam filtering, to help improve customer on-boarding and remove abusive callers from its platform.

In addition to these and other operational and technical safeguards, Twilio has adopted a strong prohibition on placing unlawful or unwanted calls through our platform. Twilio's Acceptable Use Policy expressly prohibits "[u]sing the Twilio Services in connection with unsolicited, unwanted, or harassing communications (commercial or otherwise), including, but not limited to, phone calls, SMS or MMS messages, chat, voice mail, video, or faxes."[5] This Policy provides Twilio with the legal tools necessary to take swift action against bad actors that attempt to misuse its platform.

Twilio also is actively collaborating with other stakeholders to combat unlawful robocalls on an industry-wide scale. It has participated in the development of industry standards including through its ATIS Board seat and through the IP-NNI task force.[6] Twilio also is a longtime

[5] Twilio, *Twilio Acceptable Use Policy* (May 1, 2019), https://www.twilio.com/legal/aup; *see also* Twilio, *Twilio Terms of Service* (May 1, 2019), https://www.twilio.com/legal/tos ("Don't use our services to break the laws, regulations, rules, etc., to violate these terms, to violate our Acceptable Use Policy, or to violate someone else's rights….").

[6] The IP-NNI task force, co-chaired by AT&T and Comcast, is charged with identifying common features to all IP-NNI implementations for voice service and producing specifications that define common implementation rules for SIP to SIP interconnection.

(continued…)

partner of Nomorobo, powering the technological platform that has helped consumers block over one billion robocalls.[7] In sum, Twilio recognizes that unlawful robocallers are a serious problem, and it has taken—and continues to take—concrete steps to help solve that problem.

III. THE COMMISSION CAN AND SHOULD COMBAT ROBOCALLS WHILE MAINTAINING THE INTEGRITY AND RELIABILITY OF THE PUBLIC TELEPHONE NETWORK.

In the effort to stop unlawful robocalls, consumers should not inadvertently be prevented from receiving legitimate calls that they want and need. The Commission repeatedly has recognized the need for the public telephone network to reliably transmit legitimate calls.[8] Thus, just as it is critical that we stop unlawful robocalls from cluttering our phone lines, consumers also must be assured that they will be able to place and receive the calls that they want.

Many of Twilio's legitimate services are at risk of being erroneously blocked or mis-labeled by overbroad call-blocking criteria or algorithms. For example, Twilio's APIs are used to facilitate anonymous communications, which is an important safety feature in many scenarios. Ride-share passengers on Lyft and Uber, hosts and guests on Airbnb, users of the dating website eHarmony, and victims of domestic abuse all rely on Twilio's products to communicate safely without having to disclose their phone numbers to strangers. Twilio's platform also is used for crisis communications—supporting mass notification systems so that schools, businesses, governments, and other organizations can quickly and effectively communicate in a moment of crisis. Twilio also helps legitimate businesses and banks to deliver important notifications to their customers.

---

[7] Letter from Aaron Foss, Nomorobo, and Rebecca Murphy Thompson, Twilio, to Marlene H. Dortch, Federal Communications Commission, Office of the Secretary, WC Docket Nos. 11-39, 17-97, 18-335 (Apr. 22, 2019).

[8] *See, e.g.*, *Establishing Just & Reasonable Rates for Local Exch. Carriers*, 22 FCC Rcd 11629, 11629 ¶ 1 (2007) ("[T]he ubiquity and reliability of the nation's telecommunications network is of paramount importance to the explicit goals of the Communications Act of 1934, as amended….").

Depending on the criteria or algorithms on which voice service providers base their call-blocking programs, some or all of these valuable services are at risk of being erroneously blocked or mislabeled. Indeed, even one of Twilio's own anti-robocall measures—its use of two-factor authentication (2FA) to confirm that a customer is the rightful user of a given number—could be blocked or mislabeled if a carrier's call-blocking algorithm is based on low average call duration.

This is not a theoretical concern. Microsoft has reported that a major U.S. carrier blocked over 1.2 million legitimate Skype Out calls during a three-month period.[9] Similarly, Numeracle has provided evidence demonstrating that "calls that consumers want to receive are frequently erroneously labeled as 'Scam' or 'Spam.'"[10] Further, several carriers have cautioned that analytics are not perfect and that opt-out blocking could lead to erroneously-blocked voice calls.[11]

Thus, in moving forward to allow voice service providers to block unlawful robocalls, the Commission should ensure that call-blocking programs are not used to block legitimate and wanted calls, which would undermine the public's confidence in the public telephone network.

IV. THE COMMISSION SHOULD ADOPT THE PROPOSED SAFE HARBOR FOR BLOCKING OF CERTAIN CALLS THAT FAIL AUTHENTICATION, SO LONG AS STRONG TRANSPARENCY AND REMEDIATION MEASURES ARE IN PLACE.

A. The safe harbor should apply to calls with complete attestation information that fail authentication under SHAKEN/STIR, as proposed in the NPRM.

---

[9] Microsoft, Notice of *Ex Parte* Communication, CG Docket No. 17-59, WC Docket No. 17-97, at 2 (Feb. 8, 2019).

[10] Numeracle, Notice of *Ex Parte* Communication, CG Docket No. 17-59, WC Docket No. 17-97 (May 22, 2019).

[11] *See, e.g.*, Letter from Daniel McCarthy, President and CEO, Frontier Communications to Hon. Geoffrey Starks, Commissioner, FCC (July 10, 2019) (noting the potential for "erroneous blocking" and stating that "Frontier is concerned about blocking legitimate calls without customers affirmatively accepting that risk by opting in to the service").

Twilio supports the Commission's proposal to provide a safe harbor for blocking calls that fail to authenticate under SHAKEN/STIR where complete attestation information is available—meaning "the originating provider has implemented SHAKEN/STIR and each intermediate provider in the call path accurately passes authentication information to the terminating provider"—but the call fails authentication because the attestation header has been maliciously altered or inserted.[12] Caller ID authentication through SHAKEN/STIR is an important component in the fight against unlawful robocalls, and a reasonable safe harbor will provide the protection from liability necessary for voice service providers to implement it.

The Commission is right to focus the safe harbor on calls for which complete attestation information is available. In these cases, there is a relatively high degree of confidence that where a call fails authentication, it has been maliciously spoofed.

In contrast, where a call does not reach the terminating carrier with complete attestation information, any number of benign reasons could account for failure to authenticate. Most notably, the call may originate from a carrier with a TDM-based network, or even from a carrier with an IP-based network but that interconnects with another carrier in the call chain in TDM format. Overwhelmingly, carriers with this profile serve rural areas, as the Commission heard at the summit on SHAKEN/STIR on July 11.[13] Allowing a safe harbor for calls that do not have complete attestation information thus would send an inaccurate signal to industry that it is acceptable to block calls originating from TDM networks or without IP interconnection, effectively shutting millions of rural consumers and businesses out of the nationwide telephone network.

---

[12] FNPRM ¶ 51–53.

[13] *See* Howard Buskirk and Jimm Phillips, *FCC Told Challenges Remain on Technology to Fight Robocalls*, Communications Daily (July 12, 2019).

By scoping the safe harbor to calls with complete attestation information, the Commission wisely will link the safe harbor to the progress of SHAKEN/STIR itself. That is, as SHAKEN/STIR is implemented, more and more calls will have complete attestation and thus be potentially subject to the safe harbor. The safe harbor accordingly will grow and scale with the rollout of SHAKEN/STIR in relevance and value to voice service providers.

B. The safe harbor should apply to the extent that voice service providers provide a mechanism for identifying blocked calls and remediating erroneous blocking or mis-labeling.

Twilio agrees that voice service providers availing themselves of the safe harbor should provide consumers and callers with a robust and reliable "mechanism for identifying and remedying the blocking of wanted calls."[14] These mechanisms will put consumers in the driver's seat, empowering them to choose which calls they do or do not want to receive and prevent the blocking of legitimate calls.

In considering this requirement of the safe harbor, the Commission should be guided by two principles: transparency and remediation. Put simply, transparency gives consumers the information they need to make informed decisions about the calls they receive, and remediation gives them the tools to put those decisions into practice.

First, transparency begins with the opt-out itself. If consumers do not know they are opted in to a call blocking program, they cannot reasonably be expected to exercise their opt out rights. Twilio accordingly agrees that consumers should be made aware in a plainly visible manner that their voice service provider has enrolled them in a call blocking program. To the extent that a consumer decides to opt out of that program, there should be a simple, uniform, and clear process for carrying out that decision.

[14] FNPRM ¶ 58.

Second, consumers that are in the default call-blocking program deserve access to a list of calls that have been blocked or labeled as "unwanted" or "spam" (or a similar designation). When a consumer can see the name of the individual, business, or organization associated with the blocked or labeled phone number, they can make an informed decision regarding whether they would prefer that call to be un-blocked. Voice service providers, in turn, should have a process in place to implement the un-blocking of calls at a consumer's request. Just as the Commission has long held that it is appropriate for carriers to block calls upon a consumer's request, it is reasonable for consumers to expect that carriers will deliver calls that a consumer has identified as wanted.

Third, originating callers also have an interest in transparency and remediation. It is important that callers (e.g., schools, hospitals, pharmacies) know when their calls are being blocked. This information enables legitimate callers to help remediate erroneous blocking and to respond knowledgeably to customer concerns. Twilio accordingly supports the Commission's proposal that voice service providers should send an intercept message to blocked callers and return a specific SIP response code when calls are blocked.[15] Likewise, voice service providers should respond promptly to callers' reports of erroneous blocking or mis-labeling, so that call recipients re-gain access to legitimate calls as quickly as possible.

Finally, as it did in the *Declaratory Ruling* on opt-out call blocking, the Commission should apply the safe harbor only to voice service providers that implement call blocking on a competitive- and technology-neutral basis.[16] Adopting this common-sense condition will put the implementation of SHAKEN/STIR on solid footing, so that it is unambiguously a tool for

[15] *Id*.

[16] Declaratory Ruling ¶ 35.

empowering and protecting consumers.

C. The Commission should protect all critical calls, not just calls to or from a narrower category of emergency numbers.

Twilio agrees with the Commission that "[c]ertain emergency calls must never be blocked," and it supports the Commission's proposal requiring voice service providers to maintain a Critical Calls Lists of phone numbers that are not to be blocked.[17] This protection, however, should extend not just to calls to or from 911 call centers, but also to calls intended to provide important information to the public that relates to the safety of life or property.

Twilio is intimately familiar with the importance of this broader category of critical calls, as our platform enables customers to provide urgent, safety-related updates to the populations they serve. We support mass notification systems so that schools, businesses, governments, and other organizations can quickly and effectively communicate in a moment of crisis. For example, during an active shooter emergency on a school campus, administrators can use these systems to provide life-saving instructions to students, faculty, and staff. In no case should these calls get blocked, even if for some reason they fail authentication under SHAKEN/STIR.

Developing a Critical Calls List that is broader than defined "emergency" numbers will require careful coordination between voice service providers and legitimate callers. With that in mind, the Commission should refer this matter to the North American Numbering Council (the "NANC"). This referral will enable industry and other stakeholders to work together to develop and implement a robust Critical Calls List that includes calls from schools, doctors, local governments, alarm companies, fraud and weather alerts, recall centers, hospitals, and airline alerts. The goal should be to reach a collaborative solution in which all critical calls reach their

[17] FNPRM ¶ 63.

destination, at the same time that bad actors are prevented from exploiting the Critical Calls List.

V. CONCLUSION

Twilio supports the Commission's efforts to combat unlawful robocalls and, in particular, to foster implementation of SHAKEN/STIR. By striking the right balance in a safe harbor, the Commission can put consumers back in control of their phones and ensure that the telephone network is both reliable *and* free of unlawful robocalls.

Respectfully submitted,

/s/ Rebecca Murphy Thompson

Rebecca Murphy Thompson
Head, Communications Policy
Global Public Policy and Government Affairs
Twilio Inc.
1101 Pennsylvania Ave, NW
Suite 300
Washington, DC 20004

Matthew S. DelNero
Rafael Reyneri
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, N.W.
Washington, DC 20001
(202) 662-6000

Counsel for Twilio Inc.

July 24, 2019